CLAIMS

1. In a computer system, a method for providing application security threat-modeling, the method comprising:

defining a plurality of model components to represent respective elements of an application, each model component comprising a respective set of potential security threats;

interconnecting the model components to form a logical model of the application; and

analyzing one or more of the potential security threats in terms of the model components in the logical model.

2. A method as recited in claim 1, wherein the model components comprise a module, a port, a store, or a wire.

3. A method as recited in claim 1, wherein the potential security threats comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation.

4. A method as recited in claim 1, wherein defining the model components further comprises

determining the respective security threat characteristics for a component of the model components based on the components corresponding functionality in the application.

5. A method as recited in claim 1, wherein analyzing one or more of the potential threats in terms of the model components further comprises:

selecting a particular component of the model components; and

responsive to selecting the particular component, displaying each other component of the model components that comprise at least a subset of similar potential security threats as the particular component.

6. A method as recited in claim 1, wherein analyzing one or more of the potential threats in terms of the model components further comprises:

selecting a particular component of the model components; and

responsive to selecting the particular component, displaying each other component of the model components that comprise at least a subset of similar addressed security threats as the particular component.

7. A method as recited in claim 1, wherein analyzing one or more of the potential security threats in terms of the model components in the logical model further comprises:

selecting a particular threat of the potential threats to indicate that the particular threat requires a threat mitigating implementation in a particular mode component of the model components, the particular threat corresponding to the particular model component.

8. A method as recited in claim 5, wherein selecting the particular threat further comprises identifying a priority that corresponds to the threat mitigating implementation.

9. A method as recited in claim 7, wherein selecting the particular threat further comprises identifying a desired level of strength technology with which to mitigate the particular threat.

10. A method as recited in claim 1, wherein selecting the particular threat further comprises selecting a particular technology with which to mitigate the one or more potential threats in a physical implementation of the application.

11. A computer-readable medium comprising computer-executable instructions for providing application security threat-modeling, the computer-executable instructions comprising instructions for:

defining a plurality of model components to represent respective elements of an application, each model component comprising a respective set of potential security threats;

interconnecting the model components to form a logical model of the application; and

analyzing one or more of the potential security threats in terms of the model components in the logical model.

12. A computer-readable medium as recited in claim 11, wherein the model components comprise a module, a port, a store, or a wire.

13. A computer-readable medium as recited in claim 11, wherein the potential security threats comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation.

14. A computer-readable medium as recited in claim 11, wherein the computer-executable instructions for defining the model components further comprise instructions for determining the respective security threat characteristics for a component of the model components based on the components corresponding functionality in the application.

15. A computer-readable medium as recited in claim 11, wherein the computer-executable instructions for analyzing one or more of the potential threats in terms of the model components further comprise instructions for:

selecting a particular component of the model components; and

responsive to selecting the particular component, displaying each other component of the model components that comprise at least a subset of similar potential security threats as the particular component.

16. A computer-readable medium as recited in claim 11, wherein the computer-executable instructions for analyzing one or more of the potential threats in terms of the model components further comprise instructions for:

selecting a particular component of the model components; and

responsive to selecting the particular component, displaying each other component of the model components that comprise at least a subset of similar addressed security threats as the particular component.

17. A computer-readable medium as recited in claim 11, wherein the instructions for analyzing one or more of the potential security threats in terms of the model components in the logical model further comprise instructions for:

selecting a particular threat of the potential threats to indicate that the particular threat requires a threat mitigating implementation in a particular mode component of the model components, the particular threat corresponding to the particular model component.

18. A computer-readable medium as recited in claim 17, wherein the computer-executable instructions for selecting the particular threat further comprise instructions for identifying a priority that corresponds to the threat mitigating implementation.

19. A computer-readable medium as recited in claim 17, wherein the computer-executable instructions for selecting the particular threat further comprise instructions for identifying a desired level of strength technology with which to mitigate the particular threat.

20. A computer-readable medium as recited in claim 11, wherein the computer-executable instructions for selecting the particular threat further comprise instructions for selecting a particular technology with which to mitigate the one or more potential threats in a physical implementation of the application.

21. A device comprising:

a memory comprising computer-executable instructions for providing application security threat-modeling;

a processor that is operatively coupled to the memory, the processor being configured to fetch and execute the computer-executable instructions from the memory, the computer-executable instructions comprising instructions for:

defining a plurality of model components to represent respective elements of an application, each model component comprising a respective set of potential security threats;

interconnecting the model components to form a logical model of the application; and

analyzing one or more of the potential security threats in terms of the model components in the logical model.

22. A device as recited in claim 21, wherein the model components comprise a module, a port, a store, or a wire.

23. A device as recited in claim 21, wherein the potential security threats comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation

24. A device as recited in claim 21, wherein the computer-executable instructions for defining the model components further comprise instructions for determining the respective security threat characteristics for a component of the model components based on the components corresponding functionality in the application.

25. A device as recited in claim 21, wherein the computer-executable instructions for analyzing one or more of the potential threats in terms of the model components further comprise instructions for:

selecting a particular component of the model components; and

responsive to selecting the particular component, displaying each other component of the model components that comprise at least a subset of similar potential security threats as the particular component.

26. A device as recited in claim 21, wherein the computer-executable instructions for analyzing one or more of the potential threats in terms of the model components further comprise instructions for:

selecting a particular component of the model components; and

responsive to selecting the particular component, displaying each other component of the model components that comprise at least a subset of similar addressed security threats as the particular component.

27. A device as recited in claim 21, wherein the instructions for analyzing one or more of the potential security threats in terms of the model components in the logical model further comprise instructions for:

selecting a particular threat of the potential threats to indicate that the particular threat requires a threat mitigating implementation in a particular mode component of the model components, the particular threat corresponding to the particular model component.

28. A device as recited in claim 27, wherein the computer-executable instructions for selecting the particular threat further comprise instructions for identifying a priority that corresponds to the threat mitigating implementation.

29. A device as recited in claim 27, wherein the computer-executable instructions for selecting the particular threat further comprise instructions for identifying a desired level of strength technology with which to mitigate the particular threat.

30. A device as recited in claim 27, wherein the computer-executable instructions for selecting the particular threat further comprise instructions for selecting a particular technology with which to mitigate the one or more potential threats in a physical implementation of the application.

31. A user interface for application security threat-modeling, the user interface comprising:

means for displaying and interconnecting a plurality of model components to design a logical model of an application, at least a subset of the model components comprising a corresponding set of potential security threat characteristics;

means for specifying a component of the model components; and

means for addressing one or more of the potential security threats in terms of the model components in the logical model.

32. A user interface as recited in claim 31, wherein the model components comprise a module, a port, a store, or a wire.

33. A user interface as recited in claim 31, wherein the corresponding security threat characteristics comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation.

34. A user interface as recited in claim 31, further comprising:

means for selecting a priority that corresponds to the one or more potential security threats.

35. A user interface as recited in claim 31, further comprising:

means for specifying a desired level of strength of technology with which to mitigate the one or more potential security threats.

36. A user interface as recited in claim 31, further comprising means for selecting a particular technology with which to mitigate the one or more potential security threats in a physical implementation of the application.